Amendments to the Specification:

Please replace paragraph 29 with the following paragraph:

[0029] A traditional data dictionary stores all of the information that is used to manage the objects in a database. A data dictionary comprises one or more catalogs. In this invention, a security catalog 108 is like a traditional system catalog but with two security properties: (a) It can never be updated manually by anyone, and (b) Its access is controlled by a strict authentication and authorization policy.

Please replace paragraph 30 with the following paragraph:

[0030] One example would be a table SEC_USER that records user account information. Some columns in the table store security-related information and are called security columns (or security fields). Each security field has a corresponding security flag field that specifies how the field value can be accessed (particularly updated). For example, a password field could be a security field, and its security flag could be set to "updatable by anyone with appropriate access privilege to the SEC_USER table", "updatable by the defined user only", or "never updatable by anyone". In the second case, only the user himself can change his own password.

Please replace paragraph 36 with the following paragraph:

[0036] By using a security catalog, no one is able to manipulate other users' important security information, and no one can impersonate other users without being detected and caught. When a database administrator creates a user account, besides specifying the usual account information, he must also specify some security characteristics (whether and how this account can be modified) so that a specific security policy is associated with this account. All the account information is stored in a security catalog table SEC_USER that may comprise the following columns, among others:

Please replace paragraph 57 with the following paragraph:

[0057] Referring to FIG. 2, when defining a table, a user may specify explicitly that he wants the content of some columns to be encrypted when the data are loaded. He can do this by issuing the following extended SQL CREATE TABLE statement: